UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

_____x

OUSSAMA EL OMARI,

Plaintiff,

v.

DECHERT LLP,
NICHOLAS PAUL DEL ROSSO, and
VITAL MANAGEMENT SERVICES, INC.,

Defendants.

_____x

Case No.: 23-cv-04607 (LAK)(OTW)

PLAINTIFF'S OBJECTIONS TO REPORT AND RECOMMENDATION

Scott M. Moore, Esq.
MOORE INTERNATIONAL LAW PLLC
45 Rockefeller Plaza, 20th Floor,
New York, NY 10111
(212) 332-3474
Attorneys for Plaintiff

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Federal Rules

Federal Statutes

State Statutes

TO: The Honorable District Court Judge Lewis A. Kaplan

I. PRELIMINARY STATEMENT

On June 1, 2023, Plaintiff Oussama El Omari, ("Plaintiff" or "El Omari"), simultaneously filed in this Court a complaint and motion for preliminary injunction against Defendant Dechert LLP, ("Dechert"), its private investigator Defendant Nicholas Del Rosso, ("Del Rosso"), and Del Rosso's company, Defendant Vital Management Services, Inc., ("Vital"), (the latter two parties collectively "the Vital Defendants").[1] (ECF 1, 6). El Omari alleges he learned in January 2023 that at least one of his email accounts was hacked beginning in 2017 by the Defendants during previous litigation in which they were adverse, and his confidential attorney-client email communications were viewed, copied and used by the Defendants.

El Omari alleges violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(2)(C), (Compl. ¶¶ 47-55), conspiracy to violate the CFAA, 18 U.S.C. § 1030(a), (Compl., ¶¶ 56-67), and conversion of his hacked emails in violation of North Carolina common law. (Compl., ¶¶ 68-75). El Omari's motion for preliminary injunction was to preserve the status quo to prevent spoliation in light of his discovery in January 2023 of the email tranche of his counsel's confidential attorney-client emails with El Omari on the Vital Defendants' Laptop. El Omari sought assistance from this Court to prevent the destruction and manipulation of El Omari's attorney-client email evidence discovered on the Laptop, and wherever elsewhere that evidence may be found. El Omari alleges the Laptop was originally in North Carolina where the Vital Defendants are located, but was moved to London.

[1] On 8/22/2023, El Omari and Dechert resolved the motion for preliminary injunction as to Dechert by stipulation. (ECF 29)

On June 2, 2023, Your Honor referred all "General Pretrial" and "Dispositive Motions" in this case to Magistrate Judge Ona T. Wang. (ECF 14) All subsequent proceedings and submissions were held before Magistrate Wang.

On September 7, 2023, El Omari filed his second request for injunctive relief, a motion for a temporary restraining order. El Omari submitted he learned by English court filings that, after the filing of this case on June 1, 2023, and during extensions sought by the Defendants, the Vital Defendants had been busy working to upend its obligations in this Court to preserve evidence. On 6/30/2023, the Vital Defendants had filed a claim in English courts which would destroy the evidence of how the email tranche came to be on the Laptop. The Vital Defendants were asking the English court to 1) order removal of the subject email tranche without first making a mirror image of the Laptop, and 2) by a forensic computer business of their choice – one which had previously worked for the Ras Al Khaimah prosecutor's office. (ECF 42, 42-1) El Omari asserted that the removal of the email tranche would lead to spoliation because no mirror image was to be made prior to removal, and the forensic computer business was not independent and conflicted because El Omari was previously prosecuted in absentia with involvement of that prosecutor's office.

No action was taken by Magistrate Wang in the form of a report and recommendation as to El Omari's requests for injunctive relief.

On October 9, 2023, the English court issued a written order, referencing the Vital Defendants' claim filed on 6/30/2023, (after this case was filed), and in the manner requested by the Vital Defendants, directing, among other things, the extraction and return to the undersigned of the email tranche from the Laptop by the Vital Defendants' expert. (ECF 63-1).

On February 9, 2024, the Vital Defendants' UK attorneys served on UK litigants their expert report prepared by Alvarez & Marsal, ("the A&M Report"), but to date the A&M Report has not been released to the undersigned due to the Vital Defendants' UK attorneys' assertion of confidentiality of the Report.

On March 5, 2024, the undersigned received a letter from the Vital Defendants' UK attorneys, the London law firm Rosenblatt, stating that A&M found the "Moore Data" on the Laptop. This letter stated "Alvarez & Marsal examined the Laptop and the Dedicated Media, during which they identified the Moore Data as being present." As of this date. the extraction and return of the "Moore Data" has not occurred.

On February 22, 2024, Magistrate Wang issued a Report and Recommendation recommending the grant of the Defendants' motions to dismiss. ("the Report"). (ECF 76). The Report did not include Plaintiff's motions for temporary and preliminary injunctive relief.

El Omari now files his specific objections to the Report.

II. STANDARD OF REVIEW ON A MOTION TO DISMISS

To survive a motion to dismiss under Fed. R. Civ. P. 12(b)(6), "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). A claim is facially plausible "when the plaintiff pleads factual content that allows court to draw reasonable inference that the defendant is liable for the misconduct alleged," but such inference must be "more than a sheer possibility that a defendant acted unlawfully." *Id*. (citing *Twombly*, 550 U.S. at 566). In other words, if the complaint only pleads facts that are "merely consistent" with a defendant's liability, then the complaint fails to meet the plausibility standard. *Id*. (citing *Twombly*, 550 U.S. at 557). "[O]nly a complaint that states a plausible claim for relief

survives a motion to dismiss." *Id*. at 679. For a complaint to show that the plaintiff is entitled to relief, the well-pleaded facts must allow a court "to infer more than the mere possibility of misconduct." *Id*. Determining whether a claim is facially plausible is a "context-specific task," and a court must "draw on its judicial experience and common sense." *Id*. at 679.

In evaluating a motion to dismiss for failure to state a claim, a court undertakes a two-pronged approach: "(1) identify pleadings that, because they are no more than conclusions, are not entitled to the assumption of truth; and (2) determine whether the remaining well-pleaded factual allegations, assumed to be true, plausibly give rise to an entitlement to relief." *Whiteside v. Hover-Davis, Inc.*, 995 F.3d 315, 321 (2d Cir. 2021). The court "must consider the complaint in its entirety, as well as other sources courts ordinarily examine while ruling on a motion for failure to state a claim, in particular, documents incorporated into the complaint by reference, and matters of which a court may take judicial notice." *Vengalattore v. Cornell University*, 36 F.4th 87, 102 (2d Cir. 2022) (quoting *Kaplan v. Lebanese Canadian Bank, SAL*, 999 F.3d 842, 854 (2d Cir. 2021)). Since the motion for failure to state a claim challenges the legal sufficiency of a claim, not its underlying facts, the court must look to the "four corners of the complaint to determine whether its allegations give rise to a legal claim" and "should read the complaint 'generously, and draw all reasonable inferences in favor of the pleader.'" *Podell v. Citicorp Diners Club, Inc.*, 859 F.Supp. 701, 704 (S.D.N.Y. 1994) (quoting *Cosmas v. Hassett*, 886 F.2d 8, 11 (2d Cir. 1989)). Nonetheless, the court does not need to adopt and recite "elements of a cause of action." *Twombly*, 550 U.S. at 555. Thus, the court must "accept all factual allegations as true and draw every reasonable inference from those facts in the plaintiff's favor." *Mayor & City Council of Balt v. Citigroup, Inc.*, 709 F.3d 129, 135 (2d Cir. 2013).

III. STANDARD OF REVIEW OF A MAGISTRATE'S REPORT AND RECOMMENDATION

A district court reviewing a magistrate judge's recommended ruling "may accept, reject, or modify, in whole or in part, the findings or recommendations made by the magistrate judge." 28 U.S.C. § 636(b)(1). With respect to a magistrate judge's recommendations on a dispositive motion, the Court reviews *de novo* those determinations as to which a party has objected. *Id*. ("A judge of the court shall make a *de novo* determination of those portions of the report or specified proposed findings or recommendations to which objection is made."); Fed. R. Civ. P. 72 (b)(3) ("The district judge must determine *de novo* any part of the magistrate judge's disposition that has been properly objected to.") However, "[t]o accept the report and recommendation of a magistrate judge on a dispositive matter as to which no timely objection has been made, the district judge need only be satisfied that there is no clear error on the fact of the record." *Piroleau v. Caserta*, No. 10-cv-5670, 2012 WL 5389931, at *1 (E.D.N.Y. Oct. 29, 2012). "[A]n order is contrary to law when it fails to apply or misapplies relevant statutes, case law or rules of procedure." *E.E.O.C. v. First Wireless Grp., Inc*., 225 F.R.D. 404, 405 (E.D.N.Y. 2004).

IV. OBJECTIONS

Let not the passage of time dull the "smoking gun" shock of Plaintiff's confidential attorney-client emails plead to have been discovered in January 2023 stored on adverse Defendant Dechert's private investigator's Laptop. Compl., ¶ 19. Nor let it be misunderstood that Plaintiff has in part plead injunctive remedies to identify, confine, and ultimately to destroy the stolen emails on Defendant Del Rosso's Laptop and all other storage devices of the Defendants found to contain Plaintiff's stolen emails. Compl., Remedy ¶ D. Pursuant to Section 1030(g) of the CFAA, "Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief

or other equitable relief." [emphasis added] This is lost in Magistrate Wang's Report and Recommendation.

Even though Your Honor referred "General Pretrial" and "Dispositive Motions" to Magistrate Wang, she erroneously substituted her own judgment and only prepared a report and recommendation only as to the Defendants' motions to dismiss, and not Plaintiff's motions for preliminary injunctive relief, and temporary injunctive relief specifically as to Defendants' ongoing efforts to seek extraction of the email tranche from the Laptop in the UK courts after this case was filed. ECF 6 and 42, respectively. Magistrate Wang also did not act on Plaintiff's letter motion to file an Exhibit 8, which was a second installment of new hacking leaks by "KB," this time after the briefing had closed. See ECF 70 and 70-1. Both El Omari and the Vital Defendants submitted substantial evidence incorporated into the complaint by reference to the UK litigation involving the Laptop, but none of this evidence was considered for any purpose, including jurisdiction, and should have been. *Mangiafico v. Blumenthal*, 471 F. 3d 391, 398 (2d Cir. 2006).

In the larger picture, Magistrate Wang fails to recognize the importance of the hacking of lawyer-client email communications in the functioning of a rule of law society or of the functioning of the courts in our Third Branch of Government. At the client level, Magistrate Wang did not seem to recognize how their transparency in the hands of an adversary undermines a client and their case. El Omari plead "[t]hese law emails would contain confidential information, such as El Omari's legal strategy, witnesses, evidence, and funding about the NY litigation defended by Dechert LLC." Compl., ¶ 30. In this case, the complaint alleges the Defendants had El Omari's attorney-client email communications during the entire time they were adverse in litigation with El Omari in New York, from 2016 to 2021. "The data on the

Laptop, determined to be between March 2011 and May 2021, is during the period leading up to El Omari's RAKFTZA employment termination in 2012 and subsequent NY litigation from 2016 onward. Compl., ¶ 20.

Instead, Magistrate Wang rewrote the complaint, not accepting it as true, and understated the harm of hacking attorney-client communications. "At best, Plaintiff alleges, with zero factual support, that the hacked emails were 'used by' Dechert's New York lawyers in *El Omari I*. (Compl. ¶ 39). But this also cannot be possible, because *El Omari I* was dismissed at the pleading stage." Report, p. 9.

Magistrate Wang also did not review the complaint for what it is: pleading a new hacking case with new causes of action, discovered to have occurred during the entire time of prior litigation. Instead Magistrate Wang continued throughout the Report to refer to the prior litigation between the parties as if the complaint was an amended complaint from prior litigation, which it is not.

Personal Jurisdiction

Magistrate Wang erred in finding a lack of personal jurisdiction over the Vital Defendants by not correctly applying NY CPLR § 302(a)(1). Report, p. 8. Magistrate Wang cited no case law and was mistaken in finding that "[t]he allegations in the Complaint do not satisfy either the 'transacting business' or 'tortious act' part of the statute…. There is no pleading that either a business transaction giving rise to the injury or a tort was committed by Del Rosso in New York." Report, p. 9. The Magistrate did not apply the "contracts" language at all, misapplied the "transactions" language, and did not consider the plain language of the documents incorporated into the complaint by reference, such as Defendant Del Rosso's UK testimony. The

Magistrate misunderstood that the UK testimony was incorporated into the complaint and did not consider the plain language of Del Rosso's testimony. Report, p. 9, fn 15.

El Omari asserted jurisdiction under § 302(a)(1) ("Transacts any business within the state or contracts anywhere to supply goods or services in the state"). See Plaintiff's Amended Consolidated Memorandum of Law in Opposition to Defendants Del Rosso and Vital's Motion to Dismiss and Reply in Support of Motion for Preliminary Injunction, p. 5. (ECF 56) ("Pls MOL") The court "must consider the complaint in its entirety, as well as other sources courts ordinarily examine while ruling on a motion for failure to state a claim, in particular, documents incorporated into the complaint by reference, and matters of which a court may take judicial notice." *Vengalattore*, 36 F.4th, at 102. Pls MOL, p. 2.

The complaint plead "[j]urisdiction is proper over Del Rosso because as Dechert LLP's private investigator, he is an agent of Dechert LLP. Del Rosso directed the hacking of El Omari through CyberRoot, the hacking agent in India, and reported the resulting illegal intelligence for use against El Omari in this District. Upon information and belief, Del Rosso made numerous trips to New York for personal meetings as part of his wrongful activities." Compl., ¶ 14.

El Omari pointed out "there are two specific facts adding to the complaint allegations that point to Del Rosso's business activity in the State of New York. First, Defendant Del Rosso testified at the London trial in *Azima*, in correcting his witness statement, that on the 'date I first delivered a secure drive' (Trial Testimony of Nicholas Del Rosso, Jan. 30, 2020, Day 7, 54, ln. 16, annexed as Exhibit 1 to the Declaration of Scott M. Moore, Sep. 22, 2023), 'I was flying to New York.'" (*Id*. at ln. 19) Magistrate Wang downplays and did not correctly evaluate this testimony, in light of the allegations that Del Rosso claims ownership of the Laptop found to contain El Omari's hacked emails, and he was traveling to New York to deliver a secure drive,

during the period he was engaged as Dechert's private investigator and Dechert was engaged in litigation with El Omari.

Who else would Del Rosso be delivering a secure drive to but transacting business with and providing services to Dechert's New York office and as part of his contractual relationship with Dechert's London office? All part of Del Rosso's "massive investigation" in Del Rosso's own words. See Pls MOL, pp. 5-7. Magistrate Wang put "massive investigation" in quotes, seeming to suggest it was an exaggeration by Plaintiff. Magistrate Wang did not recognize it was Del Rosso's own words from his UK testimony. Report, 9.

Statute of Limitations

Magistrate Wang erred in finding that El Omari's CFAA claims are barred by the 2 year statutes of limitations under 18 USC § 1030(g), because she misapplied the discovery of damage element of the statute of limitations and the case of *Sewell v. Bernardin*, 795 F.3d 337 (2d Cir. 2015). Magistrate Wang further factually confused the date of El Omari's discovery of the damage - which was January of 2023 when he received a notice his emails had been hacked, rather than the approximate date of the email hack, January 12, 2017. Report, pp. 11-12.

Sewell is clearly distinguishable on the facts. In application of *Sewell*, Magistrate Wang notes "The Second Circuit found that the two-year statute of limitations began to run from the date she discovered – for each account — that she could no longer access her accounts." Report, p. 10. "Here, Plaintiff discovered the intrusion in January 2017, as soon as he clicked on the link." Report, p. 12. But there are <u>no facts</u> that El Omari could not access his email accounts at the time of the hack in 2017. That would defeat the clandestine and ongoing theft.

Magistrate Wang also confused the facts and misapplies the law in her finding that "Nor is it plausible to find that the "discovery of the damage" occurred when Plaintiff received the UK

Notice in 2023, or after he conducted an investigation after receiving the UK Notice." Report, p. 12. Magistrate Wang erroneously reasoned it was not plausible because she confused the facts and improperly imputed to El Omari a duty to find hacking where he did not know it existed, and imputed a high level of hacking knowledge and sophistication by a victim not required under the statute. Magistrate Wang really implies that El Omari should have discovered the email hacking in 2017, even though in fact he did not. "[I]in his proposed Third Amended Complaint in El Omari I, Plaintiff claimed that his "computer expert" had created a document dated January 25, 2017, that indicated that his personal website had been hacked in 2014. (El Omari I, ECF 121-1 at ¶¶ 84-93)." Report, p. 12. However, this document from an earlier case, and not discussed in the briefing here, was completely unrelated in manner, time and place; it related to a 2014 hack of a website hosted in Canada, completely unrelated to the then unknown 2017 email hacking in this case.

Even if Magistrate Wang is correct that the damage discovery date was imputed to be in 2017, which she is not, that portion of the hacked email tranche on Del Rosso's Laptop which fall after that date are not barred because El Omari could not have discovered the damage of the theft of future emails. Magistrate Wang did not consider the date range of the stolen emails. The complaint alleges the stolen email tranche found on Del Rosso's Laptop ranged in date from March 2011 to May 2021. "The data on the Laptop, determined to be between March 2011 and May 2021, is during the period leading up to El Omari's RAKFTZA employment termination in 2012 and subsequent NY litigation from 2016 onward." Compl. ¶ 20. As such, the damage by the theft of emails dated after the January 2017 hack was not and could not have been discovered until the January 2023 notice, and the statute of limitations does not bar a claim for that portion of the stolen emails.

Magistrate Wang reasoning is narrow and erroneous, that "to find otherwise would nullify the limitations period in 18 USC § 1030(g), encourage a willful ignorance of phishing and other hacking techniques, and reward a lack of basic cyber security awareness." Report, p. 13. There is nothing in the statute to support this language. Nor does a plain reading of the complaint support Magistrate Wang's language of "willful ignorance" or "lack of basic cyber security awareness" on the part of El Omari. To the contrary, the complaint shows that El Omari has been unfairly undermined from the start by the clandestine intelligence gathering of the defendants which made his attorney-client communications transparent to them. The object of the CFAA, a criminal law, is to protect victims like El Omari, and hold hacking accountable.

Magistrate Wang was also mistaken in application of equitable estoppel to the Defendants' assertion of a statute of limitations defense to El Omari's conversion claim, and finding they were not estopped. Report, p. 13, fn. 19. "Plaintiff has not pleaded conduct, intent, or knowledge of the real facts." *Id*. But the real facts are that the stolen email tranche was found on Del Rosso's Laptop, in and of itself a private storage device not open to El Omari or the public.. El Omari pointed out the facts in the complaint establishing equitable estoppel. "First, the Defendants hacked into El Omari's email accounts during the NY litigation in 2017, unbeknownst to El Omari, and converted El Omari's email communications for their use. (Compl. ¶ 69) Such secretive conduct undermines basic fair play in litigation. The Defendants falsely represented themselves as being fairly involved in the NY litigation, in the sense of being officers of the court with all the duties and obligations of fair play that entails. Also, the Defendants attempted to hide their hacking efforts by urging CyberRoot to prepare false invoices, which further shows that the Defendants concealed their conduct during the NY

litigation. (*Id*. at ¶ 35) Thus, the Defendants' secret conversion amounts to a false representation or concealment of material facts.

The fact that the Defendants hacked into El Omari's email accounts and concealed their hacking efforts on a private Laptop moved out of the United States strongly suggests their intention to convert El Omari's emails. *See id*. Lastly, the Defendants had sufficient knowledge about the hacking, for they actually had the stolen emails and hired and paid CyberRoot to hack into El Omari's email accounts. (Compl. ¶¶ 32-34) Therefore, the requirements for equitable estoppel are met. Pls. MOL, pp.14-15.

Counts One and Two: Hacking and Conspiracy to Commit Hacking (18 U.S.C. § 1030(a)(2)(C))

Magistrate Wang misapplied 18 U.S.C. § 1030(a)(2)(C) to the facts in the complaint, mistakenly finding "[w]hile he provides more detail this time [referring to prior litigation], the allegations are still insufficient." Report, p. 15. Another example that Magistrate Wang rewrote the complaint.

However, first Magistrate Wang correctly found sufficiency in the complaint that Plaintiff was hacked within the meaning of the statute. "Plaintiff alleges sufficient facts that he was hacked by someone." Report, p. 16.

Then Magistrate Wang erroneously rewrote the complaint as a who dunnit mystery. "Although there is more detail about the hack itself, Plaintiff still does not plead facts to establish that Defendants – as opposed to someone else – hacked or conspired to hack his emails." Report, p. 17. "While Plaintiff pleads Defendant Vital sent over $500,000 in wire transfers to an organization in India called CyberRoot in 2015 and 2016 (Compl. ¶ 33), the rest of the allegations attempting to link Defendants to the hacking are conclusory and made "upon information and belief." Report, p. 17.

This confuses the facts, not mentioning the smoking gun – the stolen emails spanning their entire litigation history with Plaintiff, Dechert's New York adversary, were found on the Laptop of Dechert's private investigator. There is no mystery here.

Another confusion is that Magistrate Wang misunderstood Plaintiff's submission relating to the leak, during this action, of hacking materials in ECF 57-6 by KB, an anonymous person, which occurred after Plaintiff filed his original brief early before the deadline. See ECF 56. Report, p. 17, fn. 23.[2] Magistrate Wang wondered why El Omari was "sharing" the leak with the Court, regarding the pending motions and erroneously took this anonymous leak as showing "someone else" hacked Plaintiff rather than the Defendants. *Id*. But Plaintiff pointed out "[t]his evidence anonymously disclosed today… shows 1) the hacking in this case was more widespread than known by Plaintiff and the undersigned, 2) the importance of preservation of emails on the Laptop, and 3) there are multiple copies of the hacked emails." Decl. of Scott M. Moore, 9/25/2023, ¶ 4. (ECF 57) The manner in which KB leaked the materials specifically to attorneys for the Defendants, as well as Plaintiff, strongly suggests a possible motive of an out of control CyberRoot dangling its own hacking evidence in an attempt to shakedown the Defendants. "The sender copied said email to email addresses of opposing counsel in this case, as well as other counsel of record in other cases involving the Vital Defendants." *Id*., ¶ 3.

There is no mystery in the detailed complaint. El Omari plead Del Rosso's Laptop containing the stolen emails front and center, and provided other connecting dot details. Magistrate Wang does not recognize or comment on the critical importance of the surfacing of a Laptop belonging to Dechert's private investigator, Del Rosso, containing Plaintiff's emails with a date range during litigation against El Omari.

[2] Magistrate Wang referred to the first KB leak as "heavily redacted," but with leave El Omari filed the leak in a less redacted form. See ECF 64, and 64-1 to 64-7.

"On January13, 2023, just months after the last case in the NY litigation was upheld on appeal, El Omari's undersigned counsel received a foreign notice pursuant to a U.K. court order, concerning disclosure in London of the discovery of three data storage devices. ("the U.K. notice"). …One device, a laptop, was found to contain a backup copy of emails containing the email address of El Omari's undersigned counsel (smm@milopc.com). This disclosure did not include the email contents or identify any sender or recipient addresses. The evidence shows to be communications between El Omari and his undersigned attorney." Compl., ¶ 19. "The data on the Laptop, determined to be between March 2011 and May 2021, is during the period leading up to El Omari's RAKFTZA employment termination in 2012 and subsequent NY litigation from 2016 onward. Compl., ¶ 20. "Del Rosso asserted a claim of ownership of the Laptop in the U.K. litigation. Del Rosso has admitted to being a private investigator employed by Dechert LLP since approximately August 2014. *Id*. "These law emails would contain confidential information, such as El Omari's legal strategy, witnesses, evidence, and funding about the NY litigation defended by Dechert LLC." Compl., ¶ 30.

As if the linkage details of the Laptop to the Defendants alone was not enough, and it is, El Omari provided other details of the Defendants to the hacking, and its fruits found on the Laptop. The plain language of the complaint alleging specific payments totaling over $500,000 by Dechert's private investigator to a publicly known hacking organization in India, CyberRoot, during the hacking period of Plaintiff's emails and their prior litigation period. See, Compl., ¶¶ 32-39.

The only information and belief pleading, erroneously seized upon and overemphasized by Magistrate Wang, had to do with non-central allegations, such as who specifically in connection with CyberRoot took the hacking instructions from Del Rosso. "Del Rosso's hacking

instructions and related communications with CyberRoot, upon information and belief, were in part through Jain, the Indian hacking ringleader. Upon information and belief, Jain's hacking database contains both of El Omari's email addresses. Jain's database is believed to also show that Del Rosso gave Jain over 40 hacking target names." Compl., ¶ 33."Upon information and belief, Del Rosso paid further and other substantial payments to CyberRoot, Jain, and BellTrox, before and after the above period, and Del Rosso after the fact urged CyberRoot to prepare false invoices in an attempt to cover-up the true purpose of his hacking payments." Compl., ¶ 35.

Magistrate Wang erroneously focused on the absence of this minute level of detail relating to how the CyberRoot organization works, without considering the larger picture involving the Laptop, to determine the entire claim was not plausible. Report, pp. 17-18. Magistrate Wang imposed upon El Omari a requirement to essentially name names, the specific CyberRoot hacker who pushed the computer buttons for the money paid to CyberRoot. Plausibility does not require this level of detail at the pleading stage.

Magistrate Wang further erred in finding lack of details to establish damages greater than $5,000. Magistrate Wang erroneously considered the damages plead as "general," "conclusory," and "incoherent," rewriting the complaint as more of a revision or amendment involving previous cases, which it is not, rather than a new complaint pleading new facts and new causes of action. Report, pp. 18-19. Magistrate Wang further misapplied *Van Buren v. United States*, 141 S. Ct. 1648, 1660 (2021) to the complaint in concluding "[t]hese are not compensable under the plain language of the statute and *Van Buren*." Report, pp. 19-20.

The complaint's pleading of forensic computer investigation costs in excess of $5,000 alone is sufficient to establish a viable claim under the statute. At first, Magistrate Wang implied that El Omari's pleading of the costs of "forensic computer investigation" in excess of $5,000 at

paragraph 41 of the complaint to be sufficient, but then failed to plainly read the complaint that such costs were specifically incurred for the computer investigation after January 2023.

Magistrate Wang improperly rewrote the complaint, not accepting the plain facts as true, and backed off, suggesting a portion of those costs were really incurred in prior cases bringing the costs to a level below $5,000. "It is also not clear whether all of Plaintiff's "forensic computer investigation costs" would be covered, since Plaintiff claimed in 2017, in *El Omari I*, that his personal website had been hacked in 2014, and claimed in *El Omari II* that he'd given five Skype interviews (and disclosed confidential information) in 2020 to someone who had posed as a reporter for Fox News." Report, p. 18, fn. 24.

But the complaint is clear. Here, the complaint plainly states the costs in this case were incurred after January 2023. "The Laptop of Dechert LLP's investigator, Del Rosso, discovered in January 2023, has caused new and ongoing injury to El Omari beginning in January 2023. To date, El Omari's damages are in excess of tens of thousands of dollars paid to date in legal fees and costs, and forensic computer investigation costs related to investigating, assessing the scope of the hacking, and seeking to remedy the complete loss of the confidentiality of the emails." [emphasis added] Compl., ¶ 41.

As to other, non-forensic computer investigation costs plead, Magistrate Wang again misread the plain language of the complaint, and too narrowly applied *Van Buren* to bar their recovery. "The Complaint goes on to describe, in general and conclusory language, that Plaintiff suffered the "complete loss of valuable confidentiality . . . in the attorney-client communication emails pertaining to El Omari's NY litigation" (*id*. at ¶ 43), and, incoherently, "spending attorney fees and costs seeking to stop the use, dissemination of, and to restore the confidentiality of the emails on the [Del Rosso] Laptop from the Defendants." *Id*. at 42." Report, pp. 18-19. Magistrate

Wang concludes "[t]he technological harm here was the apparent malware installation on Plaintiff's computer systems, and the Complaint does not sufficiently allege that the costs Plaintiff suffered were "from efforts to identify, diagnose, or address [that] damage." (El Omari II, ECF 95 at 44). Instead, he has continued to include the "value" of the confidentiality of Plaintiff's 2017 emails and efforts (including litigation) to "restore the confidentiality"[25] of the emails in his pleading of loss. These are not compensable under the plain language of the statute and *Van Buren*.[26]

> [25] It is further unclear what Plaintiff means when he seeks to "restore" confidentiality of the emails that were copied. The emails were disseminated to many, and that bell cannot be unrung. Restoring the security of his email accounts might have included changing passwords and other security measures after he clicked on the link, but it would be unreasonable to read the statute to mean that. In the 7 years since that incident, Plaintiff and his counsel (as well as counsel for defendants) have received emails from an anonymous "KB" who claims that all of Plaintiff's and his counsel's email accounts have been compromised. (*See* ECF 57-6). If that is true, then the destruction of emails on the Del Rosso Laptop would have no effect on "restoring confidentiality" of any communications that had been copied and disseminated since 2017. [emphasis added]
>
> [26] Plaintiff quotes from *Van Buren*'s dicta about technological loss, and omits the last sentence, which makes clear that the "loss of privilege of" Plaintiff's emails is not recoverable damage. *Van Buren* examined whether a police officer could be held criminally liable for using information from a law enforcement database for a personal (and hence improper) purpose. In holding that he could not, the Supreme Court noted that the statute's definitions of "damage" and "loss" focused on technological harms from the hacking itself (the quoted language in Plaintiff's brief), to then say, "[t]he term's definitions are ill fitted, however, to remediating 'misuse' of sensitive information that employees may permissibly access from their computers. Van Buren's situation is illustrative: His run of the license plate did not impair the 'integrity or availability' of data, nor did it otherwise harm the database system itself." 141 S. Ct. at 1660 (internal citations omitted)." [emphasis added]
>
> Report, pp. 19-20

There is nothing incoherent in the pleading. Magistrate Wang's footnotes are important and are mistaken in fact and reasoning. Footnote 25 of the Report questions El Omari's use of

the word "restore" in damage paragraph 42 of the complaint, and reads things into the complaint that are not there. That paragraph reads "… monetary expenses of investigating the hacking and spending attorney fees and costs seeking to stop the use, dissemination of, and to restore the confidentiality of the emails on the Laptop from the Defendants." [emphasis added] Compl., ¶ 42.

Magistrate Wang is wrong and her analogy does not apply here, when she says, "The emails were disseminated to many, and that bell cannot be unrung." Report, p. 19, fn. 25. The complaint does not state that the hacked emails "were disseminated to many" which implies a public release, although there may be "many" within the circle of the Dechert law firm. Aside from the hacker in CyberRoot, the complaint states one known person had access to the hacked emails, Del Rosso, Dechert's private investigator, on his Laptop, and the information from the emails were disseminated to Dechert. This is a discrete number, identifiable, containable, and destroyable. "Confidential and privileged email communications between El Omari and his undersigned attorney were copied from El Omari's email account and disseminated for use [by Dechert] against him in the NY litigation… it is presently unknown how many other copies of the illegal email tranche may exist and who possesses them. These law emails would contain confidential information, such as El Omari's legal strategy, witnesses, evidence, and funding about the NY litigation defended by Dechert LLC." Compl., ¶ 30. Persons within Dechert who would have had access or information from the stolen emails would be Linda Goldstein at Dechert NY who defended against El Omari, and any other Dechert counsel of record or staffer who worked on the cases. Compl., ¶ 9.

The only known copy of the stolen email tranche is on Del Rosso's Laptop, although there may be other copies, or information about the email tranche in reports or other form by Del

Rosso, within Dechert's circle. "The timing of the Laptop manufacturing date which predates the emails contained thereon indicates that the illegal email tranche in "update24Jan.rar" on the Laptop was copied from another source in 2019 or later and is itself a copy." Compl., ¶ 20. Thus there is one finite known person and place, Del Rosso's Laptop, which can be contained, isolated and the email tranche ultimately destroyed. This "restores" the confidentiality of this stolen email tranche. The same identification, containment, isolation and destruction can be done in the event other copies of or information about the email tranche are found to exist by Del Rosso or in the Dechert law firm. This "restores" confidentiality. El Omari's remedy plea in the complaint includes this relief. "Ordering that, after issuance of a final, non-appealable judgment in this action and then only with the express permission of this Court of Plaintiff, Defendants to destroy all the information obtained from Plaintiff as a result of the alleged wrongdoing in their possession, custody or control." Compl., Relief, ¶ D.

Magistrate Wang's footnote 26 in the Report shows she misapplied the damage limitations in *Van Buren*. Magistrate Wang's concluded that Plaintiff's argument that the requested relief is permitted by *Van Buren* is undercut by a subsequent sentence in the opinion. "Plaintiff quotes from *Van Buren*'s dicta about technological loss, and omits the last sentence, which makes clear that the "loss of privilege of" Plaintiff's emails is not recoverable damage." Report, p. 20, fn. 26. El Omari argued that "The aforementioned stealing of data, or a data breach, and El Omari's remedial efforts to determine the extent of the data loss, retrieve and preserve their confidentiality, is a covered "cost of responding to an offense," a typical consequence of hacking, within *Van Buren. See* 18 U.S.C. § 1030(e)(8)." Pls MOL, p. 23.

But Magistrate Wang quotation of the next sentence in *Van Buren* does not apply as she reasons, "[t]he term's definitions are ill fitted, however, to remediating 'misuse' of sensitive

information that employees may permissibly access from their computers. Van Buren's situation is illustrative: His run of the license plate did not impair the 'integrity or availability' of data, nor did it otherwise harm the database system itself." 141 S. Ct. at 1660 (internal citations omitted)." Report, p. 20, fn. 26.

In relying on this language, Magistrate Wang erroneously concludes that El Omari's complaint damages involve seeking to remediate the "misuse" of the stolen attorney-client communication emails. Well, the Defendants' "misuse" of the stolen data in past litigation is indeed a bell that cannot be unrung, but restoring the confidentiality of the stolen data can be since there is alleged a finite circle within which the stolen data exists and can be identified, contained, and destroyed.

The difference is in the facts, Van Buren accessed a database and did not "impair the 'integrity or availability' of data, nor did it otherwise harm the database system itself." Here, Magistrate Wang correctly concluded El Omari's database was harmed by the malware. "Plaintiff alleges sufficient facts that he was hacked by someone…." Report, p. 16. The harm from the malware and the newly identified copy of the stolen email tranche on Del Rosso's Laptop, is the direct link to "El Omari's remedial efforts to determine the extent of the data loss, retrieve and preserve their confidentiality, and is a covered "cost of responding to an offense," a typical consequence of hacking, within *Van Buren. See* 18 U.S.C. § 1030(e)(8)." Pls MOL, p. 23.

Count Three: Conversion

Finally, Magistrate Wang erred in concluding that "Count Three – conversion under North Carolina law – is both time barred and fails to state a claim." Report, p. 20.

Magistrate Wang erred in application of the North Carolina statute of limitations in concluding "the discovery rule does not apply to conversion claims under North Carolina law, and the "hack" occurred in January 2017." Report, p. 20.

But Magistrate Wang did not review or consider El Omari's argument, that the statute of limitations did not even begin to run until January 2023 because all the statute's elements had not been met until that point. This is an argument not involving the discovery rule. "The § 1-52(4) clock did not start running until January 13, 2023. Although the hacking occurred in 2017, the "dominion" over the subject emails on the Laptop was of a hidden and secret nature. The "exclusion" of El Omari's rights to the subject emails on the Laptop never occurred until he knew by the notice from the U.K. litigation they were on the Laptop on January 13, 2023. (Compl. ¶ 19) El Omari could not be excluded from the subject emails if he didn't know they were on the Laptop. On that date, January 13, 2023, El Omari began to be excluded from the subject emails on the Laptop, and all the elements of conversion were met on that date." Pls MOL, p. 12. El Omari's emails are still on the Laptop and he remains excluded from them since 2023.

Magistrate Wang did not consider application of the discovery rule under more recent case law. Report, p. 20. See, Pls. MOL, p. 13. "However, the entire principle upon which defendants' argument hinges, which is that the statute of limitations begins to run against a plaintiff who has no way of knowing that the underlying breach has occurred, runs afoul of both our recent decisions, such as *Christenbury*, and basic notions of fairness. *Chisum v. Campagna*, 855 S.E.2d 173, 188-89 (N.C. 2021).

As pointed out above at page 9, Magistrate Wang also misapplied estoppel. See also, Pls. MOL, p. 13.

Magistrate Wang also erred in application of the elements of the North Carolina conversion law in concluding that emails cannot be converted. "Plaintiff has not sufficiently pleaded that a conversion occurred." Report, p. 20. "The North Carolina Supreme Court has defined the tort of conversion as "an unauthorized assumption and exercise of the right of ownership over goods or personal chattels belonging to another, to the alteration of their condition or the exclusion of an owner's rights." *Variety Wholesalers, Inc. v. Salem Logistics Traffic Services, LLC*, 365 N.C. 520, 523 (N.C. 2012) (internal citation omitted). Emails are neither goods nor personal chattels, and Plaintiff's use of his email account apparently continued unimpeded." *Id*. (Magistrate Wang included a footnote in this sentence citing *Van Buren*, but *Van Buren* did not purport to interpret North Carolina conversion law or its elements.)

But Magistrate Wang did not review or consider El Omari's federal case law that denial or violation of the plaintiff's dominion over or rights in property is an act of conversion. ""Under North Carolina law, "'[c]onversion is defined as: (1) the unauthorized assumption and exercise of the right of ownership; (2) over the goods or personal property; (3) of another; (4) to the exclusion of the rights of the true owners.'" *TSC Research, LLC v. Bayer Chemicals Corp.*, 552 F.Supp.2d 534, 542 (M.D.N.C. 2008) (quoting *Eley*, 171 N.C. App. at 371). North Carolina law allows a claim for conversion to be premised on something other than *just* the denial of the rights to the property. "'[T]he general rule is that there is no conversion until some act is done which is a denial *or violation of the plaintiff's dominion over or rights in the property*.' Thus, Defendants' conduct did not need to completely deprive Plaintiff['s] use and access to its computer files as Magistrate Wang reasoned. It would be sufficient if Defendants' conduct violated Plaintiff's dominion or control over the property (here, the computer files), or if Defendants altered the condition of Plaintiff's rights to those computer files." (internal citations omitted) (emphasis in

original). *Bridgetree, Inc. v. Red F Marketing LLC, et al*, No. 3:10-CV-00228-FDW-DSC, Doc. No. 253, at 26 (W.D.N.C. Feb. 5, 2013). Here, El Omari's exclusive and confidential rights—i.e., dominion over and rights—in his hacked email communications, has been lost. This constitutes a "denial *or violation of the plaintiff's dominion over or rights in the property*" and a properly plead conversion claim. " Pls. MOL, p. 16.

V. REQUEST TO AMEND THE COMPLAINT

In the event that Magistrate Wang's recommendation is accepted, which it should not, El Omari respectfully requests an opportunity to amend the complaint under Fed. R. Civ. P. 15(a)(2) to cure any pleading defects. El Omari has not previously requested, nor has there previously been any amendments to the complaint.

VI. CONCLUSION

FOR THE FOREGOING REASONS, PLAINTIFF OUSSAMA EL OMARI respectfully requests this Honorable Court to REJECT the Report and Recommendation dated February 22, 2024 recommending this case be dismissed in its entirety. (ECF 76). In the event the Report and Recommendation is accepted, which it should not, Plaintiff respectfully requests an opportunity to amend the complaint.

Dated: New York, New York
March 7, 2024

Respectfully submitted,

MOORE INTERNATIONAL LAW PLLC.

/s/ Scott M. Moore
By: _____
Scott Michael Moore, Esq.
Attorneys for Plaintiff, Oussama El Omari
45 Rockefeller Plaza, 20th Floor
New York, New York 10111
T. (212) 332-3474